National Audit Office
Notre Dame Ravelin
Floriana FRN 1600
Malta

Phone: (+356) 22055555
Fax: (+356) 21220708
E-mail: nao.malta@gov.mt
Website: www.nao.gov.mt

Auditor General

Our Ref: NAO 69/2011
Your Ref:

20 ta' Jannar, 2014

Is-Segretarju
Kumitat Permanenti dwar il-Kontijiet Pubblici
Il-Palazz
Valletta

Rigward: Talba mill-Kumitat Permanenti dwar il-Kontijiet Pubblici

B'referenza għat-talba tal-Onor. Owen Bonnici mressqa permezz ta' korrispondenza datata 9 ta' Novembru, 2013 u diskussa waqt il-laqgħa tal-Kumitat Permanenti dwar il-Kontijiet Pubblici tat-13 ta' Novembru, 2013, l-Uffiċċju Nazzjonali tal-Verifika qiegħed jippreżenta risposta f'dan ir-rigward wara konsultazzjoni mal-Malta Information Technology Agency (MITA).

L-informazzjoni provduta mill-MITA hija annessa ma' din l-ittra.

Dejjem tiegħek,

A. C. Mifsud

Kopja lil: Chairman, MITA

Ref	NAO Query	Feedback from MITA
1	The user has a certificate assigned he can log on with the certificate WITHOUT knowing the password;	MITA does not make use of 'certificate based' authentication.
2	If the user has a delegate assigned that delegate can simply open the Inbox WITHOUT knowing the password;	Delegates are explicitly assigned by the owner of the respective mailbox. The delegates use their password to access their mailbox and to those to which they were explicitly delegated access to.
3	If the mailbox permissions are not correct someone can just open the Inbox WITHOUT knowing the password;	Users are required to key in their respective password prior to mailbox access, irrespective of assigned permissions. Mailbox permissions are assigned according to the request(s) logged by clients via the MITA eRFS system. MITA provides Ministry CIOs with a quarterly report that details permissions assigned to (generic and personal) mailboxes owned by the respective Ministries and Entities to ensure so that they have visibility on permissions assigned.
4	Administrators can open the Mailbox without having the password;	Administrative roles with administrative privileges in this particular operating and product construct, by design, allow this. The MITA Email service is configured with the following configuration: *'Administrators have an explicit deny to open mailboxes'*. Access is governed through the following MITA Access Control Policy statement *"Everything is generally forbidden unless expressly permitted"*. MITA administrators are security screened every three (3) years by the Malta Secret Service.
5	There could be a shadow box configured and a different user opens the shadow box;	In order to provide concrete feedback, it would be beneficial if the NAO can clarify what is being referred to by the term 'Shadow Box'.
6	Interception of email via SMTP Sink at the network perimeter;	This is believed not necessarily specific to mailbox access – in general (*applies to 1-8*), MITA performs: Internal security audits External penetration tests by approved third parties Implements best practices and policies, with relevant controls (*technical or otherwise*) in place Is fully ISO 27001 certified